Privacy Impact Assessment for

Box Secure File Transfer Production (Box)

September 8, 2025

Contact Point
Joseph Powers
Associate Chief Information Officer
OCIO/Enterprise Infrastructure Systems (EIS)

Reviewing Official
Becky Ronayne
Senior Agency Official for Privacy

Abstract

OPM currently has numerous secure file transfer solutions but no enterprise-wide solution that meets a wide range of customer requirements while remaining security compliant. The Box Secure File Transfer (SFT) solution establishes a mechanism to securely transfer files with entities external to OPM guided by established security policy governance. This PIA is being conducted because personally identifiable information will potentially be transmitted using Box.

Overview

Currently, OPM does not have an enterprise-wide tool available to securely transfer data (PII and non-PII) to OPM or from OPM. As a result, different OPM offices have acquired different Secure File Transfer (SFT) tools that, in some cases, are not available to all users/program offices. Other program offices burn data to CDs and mail them to external users.

Early in 2022, OCIO created a task force/working group to evaluate this issue and recommend an enterprise-wide solution. The task force solution, Box SFT (Box), was successfully piloted in 2022.

The new SFT production solution will be available to users across OPM and ensure data transfers to and from OPM are secure, auditable, and efficient. Each OPM licensed-user will have a Box account, accessed via Single Sign-On (SSO) with their Microsoft 365 account, which relies on PIV authentication. Box will prompt file recipients and remote senders of files to OPM to create their own Box accounts (with multifactor authentication). The data that will be approved for external sharing or receipt, includes information such as annuitant information and shared inter-agency work products.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Information transmitted by Box is authorized under various authorities and/or agreement; any inquiries as to the authority must be referred to the appropriate Program Office. Each Program Office that uses Box has the legal authority via a license from Box to administer and use Box to transmit information outside of OPM in conjunction with their responsibilities. This includes technical support by the USA suite of tools, transferring information to/from annuitants, and exchanging policy documents with other agencies. All the data transfers occur today via email, mailing of CDs, and the use of alternate SFT systems.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Personal identifiable information that is transferred using Box is covered by the SORN applicable to the system of record in which the information is maintained. No general SORN(s) apply to this wide range of information.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes, Box has a system security plan. The Collaboration Tools Authority to Operate was last signed on February 7, 2024. Box is a subsystem of Collaboration Tools.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. This system is not intended as a permanent repository but rather a way to transfer files to/from external agencies and the public. The files shared via Box will only remain for up to 30 days before they are deleted.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not applicable since Box is not designed around the collection of any specific information or form.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

Each Box user will provide their name and email address to acquire an account; some users may also provide their phone number for multifactor authentication. This is the extent of the information that is specifically requested and retained in Box.

Box will also collect and disseminate a broad range of documents that were created by OPM or elsewhere and then needed to be sent to another user who may be within or elsewhere. This information will only remain in Box for up to 30 days before it is deleted.

2.2. What are the sources of the information and how is the information collected for the project?

Box will collect information from OPM staff, plus individuals outside OPM who could be members of the public or staff from different organizations. They will use Box to upload and send non-classified sensitive information to, from, or within OPM.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Box is a transport infrastructure that does not exercise control over the contents of records shared in the system.

2.4. Discuss how accuracy of the data is ensured.

Box is strictly a tool used to transfer sensitive information which comes from other sources or individuals. It is the responsibility of the individual using Box to ensure that they feed accurate information into Box.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that the system will collect and maintain more information than is relevant and necessary to accomplish the agency's mission.

Mitigation: This risk is partially mitigated. Box is a transport infrastructure that does not exercise control over the contents of records shared in the system. Therefore, Box does not analyze the contents of records in the system. On the agency side, OPM's authorities and procedures ensure that there are limits on the types of information that OPM may request or send via Box. For example, OPM will not transmit classified materials via Box. Additionally, OPM provides the statutory protections afforded under the Privacy Act, along with the privacy tenets in the Fair Information Practice Principles, and strives to only collect personal information that is necessary to accomplish the agency's mission.

Privacy Risk: There is a privacy risk that information will be collected without the proper legal authority.

Mitigation: This risk is partially mitigated. OPM's internal policies mandate that Box users may only transmit or receive information that is authorized by statutes, regulations, or other authorities, and only for purposes to assist in the performance of agency responsibilities and to conduct the agency's mission. These authorities may be found generally in this PIA and in OPM's SORNs governing the type of information being transmitted

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

OPM and its agency partners will use the system to transfer files securely, efficiently, and in an auditable (traceable) manner to/from external agencies and the public.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

No.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Participating OPM program offices will manage their respective licenses and be responsible for using those licenses. OPM OCIO personnel will administer BOX, view logs, resolve issues with user accounts, etc.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information sent by the system will be used inappropriately.

Mitigation: This risk is partially mitigated. OPM has implemented several measures to ensure that OPM Box users handle information in accordance with the uses described above. Users are approved for an account by their office director to ensure that only OPM employees requiring a Box account receive one for the performance of their official duties. Box's built-in controls limit access to the user's account to ensure that the information is available only to individuals who have the authority to access the information. Additionally, all files and folders are associated with a specific user, and each user has specific permissions associated with the information in their account, which specify how a user may interact with a particular file. Every time a user attempts to access a file or folder, Box uses these permissions to verify that a user has explicit authorization to interact with the file. This

process ensures that access is restricted to the authorized type of interaction with those specific files or folders.

Box audit logs are available on a read-only mode to OPM's Box Administrator. That individual has the capability to review Box audit logs for security monitoring, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Box audit logs are automatically monitored by Box's Security information and event management (SIEM) tool. Any alteration of Box audit logs is flagged by SIEM, which sends a notification to OPM's Box Administrator. This ensures that OPM's Box Administrator is alerted to any unauthorized alterations of the audit logs. Files securely shared via Box are deleted after 30 days through automated means.

In addition, each office with a Box account can further customize the security and permissions associated with its files. For example, OPM offices with a Box account can determine how users in their office may access records in the account. OPM offices may also specify other limitations, such as limiting access only to users with an opm.gov email address or prohibit downloading a certain file. Overall, Box users are given only the privileges they need to access a file, and the file is deleted through automated means. Additionally, OPM's Box Administrator can automate functionality that will place records into a restricted "Quarantine" area if they meet certain parameters, such as records containing social security numbers or specific words or phrases that may indicate a level of protection higher than Controlled Unclassified Information (CUI). When this functionality is enabled, OPM's Box Administrator must review and take action to release these records from the Quarantine area before they are accessible to OPM Box users.

Privacy Risk: There is a risk that users could use information received from the system for purposes other than that for which the information was provided.

Mitigation: This risk is partially mitigated. The OPM Box user determines the recipient(s) who may access the records through an invitation or web address. Additionally, OPM communicates applicable restrictions on further dissemination of the records as a part of the release of the information. For example, information released under a routine use in an OPM SORN is restricted from disclosure outside of the stated uses approved by OPM's privacy office. Other records, such as records released in response to a FOIA request, constitute public information and do not require additional protections.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Box does not provide notice to individuals. The only information collected directly by Box is that which the vendor needs to set up the account; specifically name and email address. Any notice provided beyond the account setup information would be provided to individuals via a notice sent through Box or another method.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Users consent to provide information to Box by setting up an account and decline by not setting up an account. External agency/public users do not need to create an account, but that will prevent them from sending or receiving files from OPM.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that Box users will not be given the opportunity to consent to the uses of their information.

Mitigation: Individuals must sign-up for a Box account to access the records. Individuals will be able to decline consent by not opening a Box

account. Additionally, to provide transparency and allow Box users to understand how their communications and other information are handled, the following measures are in place:

- OPM's security-warning banner on the Box login screen informs users that any information they transmit through Box, may be monitored, intercepted, searched, and seized by the agency.
- Links to the Box Privacy Policy and Terms of Use are displayed in the footer of every page in the Box system.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

Each Box user will have to provide their name and email address to acquire an account; some users may also provide their phone number for multifactor authentication. This is the extent of the information that is specifically requested and retained in Box.

The information in the files sent via Box will vary depending on the program (such as bank statements, proof of employment, USA Staffing, etc.). This system is intended for the temporary storage of documents while they are being sent to or received from external users.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information collected by the system may be retained longer than necessary.

Mitigation: This risk is partially mitigated. OPM applies NARA-approved records retention schedules to files submitted through Box. Records transmitted through Box are deleted after 30 days through automated means. Box audit logs of administrative information maintained by OPM are deleted after 30 days unless there is a business use which requires a longer retention.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

BOX is the system OPM uses to facilitate the secure sharing of files with external agencies and/or the public. Therefore, OPM employees will share and receive sensitive information via Box as needed.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Personal identifiable information that is transferred using Box is covered by the SORN applicable to the system of record in which the information is maintained. No general SORN(s) apply to this wide range of information.

6.3. Does the project place limitations on re-dissemination?

No. There is not a way to control files once they are sent to external users. Files received from external users will be controlled on the OPM side but not from the user side.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The system has audit logs that show file activity (sent or received).

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information will be shared outside the scope of the applicable SORN or without the proper authority or accounting.

Mitigation: This risk is partially mitigated. All OPM Box users are required to complete annual privacy awareness training, which informs users on their Federal information privacy requirements, including the proper handling of PII. External parties provided PII under a routine use are subject to Privacy Act limitations on disclosures. Any use of the records must be compatible with the purpose of the collection, as outlined in the applicable SORN. Other records, such as records received pursuant to a FOIA request, constitute

public information and OPM has no authority to limit the re-dissemination of records released under a FOIA request.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

Users can view their profile. They can also see the files that are available to them (e.g., what they are sharing or accepting from others).

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The only information stored about each user is their name, email address, and possibly phone number. This information is under the user's control via their profile.

7.3. How does the project notify individuals about the procedures for correcting their information?

This is covered in the vendor's documentation on how to use Box.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: Box is not the system of record for information passed through it, therefore individuals must contact the appropriate Program Office which owns the system of record for which the information was originally collected to address any discrepancies with respect to the accuracy of information passed via Box.

Mitigation: Not applicable.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

Actions are logged and ingested in OPM's Microsoft Defender for the Cloud environment.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

There is extensive vendor documentation. There will also be training sessions for all OPM users. This is not specifically privacy training but will cover any relevant privacy topics.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Individual users' control who they send files to and whom they request files from. Administrators can see a list of users to troubleshoot issues. Administrator access is controlled via a special Azure Identity Access Package.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The project team would review additional capabilities beyond the transmitting of documents. There are no MOUs or other external agreements.

Responsible Officials

Joseph Powers
Associate Chief Information Officer
OCIO/Enterprise Infrastructure Systems (EIS)

Approval Signature

Becky Ronayne
Acting Senior Agency Official for Privacy